UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-v-

LAWRENCE RAY,

Defendant.

20-cr-110 (LJL)

OPINION & ORDER

LEWIS J. LIMAN, United States District Judge:

Defendant Lawrence Ray ("Ray") moves to suppress evidence obtained from a computer seized, pursuant to warrants, at the house of his father (the "Premises" or "Apartment") on or about July 22, 2021. On July 21, 2021, the government received a warrant (the "Premises Warrant") to search the residence of Mr. Ray's father in Staten Island and seize a silver 17-inch Macbook Pro (the "Computer") used by Mr. Ray, and on July 23, 2021, after seizing the Computer from Mr. Ray's father's house the prior day, the government received a second warrant (the "Computer Warrant") to search the entirety of his Computer. Ray moves to suppress the evidence obtained from the Computer on the grounds that there was an insufficient nexus between the seized Computer and the probable cause asserted in the Premises Warrant and that the Computer Warrant was overly broad and non-particularized. Ray recognizes that the challenges he makes are similar to those raised and rejected in Ray's prior motion to suppress evidence seized pursuant to warrants. Familiarity with the Court's prior opinion at Dkt. No. 184 is assumed. Based on substantially the same principles discussed in the Court's prior opinion, Ray's motion is denied.

BACKGROUND

The seizure of the Computer was effectuated through two warrants. The Premises Warrant was obtained on July 21, 2021. It authorizes law enforcement to search an apartment belonging to a person identified in the warrant application only as the Relative, but who all acknowledge now is Ray's father, and to seize the Computer and to search it for evidence of the crimes charged in the superseding indictment (the "Indictment"). The affidavit in support of the Premises Warrant was sworn by Special Agent Kelly Maguire ("SA Maguire"), the Federal Bureau of Investigation Special Agent who signed most of the affidavits in support of the warrants discussed in the Court's prior opinion. The affidavit attaches the Indictment returned against Ray and Isabella Pollok ("Pollok"), Dkt. No. 127, and provides probable cause from that Indictment that Ray engaged in the federal crimes of RICO conspiracy, forced labor, trafficking with respect to and conspiracy to commit forced labor, and sex trafficking, as well as money laundering, extortion, and tax evasion. Among other allegations, the Indictment charges that Ray, Pollok, and others extracted false confessions from their victims, including an individual identified as Female Victim-1, and used those false confessions to extort money from the victims, to force some of the victims to perform unpaid manual labor, and to cause Female Victim-1 to engage in commercial sex acts for the benefit of Ray, Pollok, and others.

The affidavit also provides probable cause to believe that evidence of the crimes of Ray and Pollok would exist in digital and/or electronic form. Among other things, Ray, Pollok, and others documented the victim's false confessions and retained at least some of them in digital or electronic form. SA Maguire describes data reviewed from Ray's email accounts (pursuant to a warrant) which contains emails attaching and/or forwarding the false confessions and other sensitive, humiliating, and incriminating material. SA Maguire further describes information

reviewed on the electronic devices contained in Ray's residence on the day of his arrest that include videos of interrogations of the victims of the offenses charged in the Indictment, as well as incriminating information and evidence of the crimes charged in the Indictment found in Pollok's iCloud account. The filenames of certain attachments and recordings reflect that the material originated and/or was maintained on an electronic device. Next, the affidavit provides probable cause to believe that the Computer, described as the "Subject Device," would contain evidence of the criminal activity charged in the Indictment and is itself evidence and an instrumentality of criminal activity. SA Maguire describes a conversation she had with Female Victim-2 on May 21, 2021; Female Victim-2 was with Ray at Ray's residence at the time of his arrest and lived at that residence. Female Victim-2 conveyed that Ray used the Computer "all the time" within his residence and brought the Computer to his bedroom before going to sleep at night; that she observed Ray using the Computer to, among other things, record "confessions" from the victims; and that she was present when law enforcement searched Ray's residence at the time of his arrest, that law enforcement did not discover the Computer, and that Pollok told Female Victim-2 that she found the Computer wedged between Ray's bed and bedside table within the residence after law enforcement left the Premises. Female Victim-2 saw Pollok take the Computer and bring it to her bedroom; a few days after the arrest, Pollok and Female Victim-2 brought the Computer to Ray's father's apartment. Female Victim-2 stated that she was last at the father's apartment on December 21, 2020 and, while there, saw the Computer inside a black laptop bag in the living room.

Probable cause to believe that the Computer would be at the Premises and that it would contain evidence of the crimes charged in the Indictment was corroborated by review of audio recordings of Ray from the Metropolitan Correctional Center to his father in June 2020 (after

Ray's arrest). In those calls, Ray tells his father that "we need to index the evidence" and "[w]e need to categorize the evidence," and makes reference to the fact that the evidence includes digital evidence of the confessions of Female Victim-1.[1]

The Premises Warrant application seeks authority to seize the Computer for later review including by conducting a file-by-file review by opening or reading the first few pages of a file to determine its precise contents and whether it contains evidence or the fruits of the crimes charged in the Indictment. The application further states that law enforcement will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. But it does not limit law enforcement to the use of search terms.

The Computer Warrant was signed on July 23, 2021 and authorizes law enforcement to search the Computer for evidence of the crimes charged in the Indictment. The affidavit in support of the Computer Warrant also is signed by SA Maguire. It includes all of the same information that is in SA Maguire's affidavit in support of the Premises Warrant. It also adds that during the execution of the Premises Warrant, SA Maguire asked Ray's father (identified again as the "Relative") where he kept the Computer provided to him by Isabella Pollok and that the father pointed to a black bag on the floor of the living room of the Apartment. The black bag contained the Computer, which was in a white rubber case wrapped in tinfoil. Ray's father stated that Pollok had provided him the bag containing the Computer and that he had not touched it since then. The Computer Warrant application also stated that when SA Maguire connected the Computer to a power source at the FBI, she observed that it was password protected and

[1] The warrant application also provides evidence that the premises to be searched are those of Ray's father, including that the Premises are his listed address, and his name was listed on the posted tenant list.

locked but that its home screen displayed an icon of a lion's head and the name Lawrence Ray, above which was a password protected field.

DISCUSSION

Ray argues first that the Premises Warrant does not establish probable cause to believe that fruits, instrumentalities, and evidence of Ray's alleged crimes would be located at the Premises because it was signed on July 21, 2021, seven months after Female Victim-2 said she last saw the black computer bag in December 2020 and almost a year and a half after she said she saw the Computer at the Premises in February 2020. He argues that the warrant application provided no detail suggesting that the black computer bag was distinctive or that Female Victim-2 had ever seen Ray use a black computer bag for his device; on the contrary, she had seen Ray store the Computer in a "white rubber" case. Ray argues it was not reasonable to assume that the computer seen by Female Victim-2 was in the black bag she saw seven months ago. Ray also argues that the June 2020 recorded jail calls between Ray and his father discussing a need to "index" and "categorize" the "evidence" does not support an inference that the Computer was still in Ray's father's possession because the calls make no reference to the Computer. In Ray's telling, the content of these calls is best understood to refer to the documents produced by the government in discovery.

Ray also argues that the Premises Warrant and the Computer Warrant allowing a "complete review of all the ESI from seized devices or stage media if necessary to evaluate its contents and to locate all data responsive to the warrant" were overbroad and not sufficiently particular. The contents of the Computer allegedly included both privileged and irrelevant information dating back to the 1990s, including information regarding phone calls and letters between Ray and his attorneys, lists of his medical records, and unrelated books. Ray argues that

the government was in a very different position with respect to the warrant application in July 2021 than it was when Ray was first arrested but that the warrants authorized law enforcement to conduct a search in a similar manner. By July 2021, the government was deep in its investigation and knew the names of people believed to be victims and those believed to be coconspirators; in addition, Female Victim-2 herself stated that the information on the Computer was well organized in "separate files" for different people with "corresponding folders" and Ray had given "instruction" "on best practices for digital folder structuring."[2]

Ray's arguments lack merit. First, Ray lacks standing to challenge the search of the Premises. "Fourth Amendment rights are personal rights [that] may not be vicariously asserted." *United States v. Haqq*, 278 F.3d 44, 47 (2d Cir. 2002) (quoting *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978)). A defendant's Fourth Amendment rights are violated "only when the challenged conduct invaded *his* legitimate expectation of privacy rather than that of a third party." *United States v. Payner*, 447 U.S. 727, 731 (1980); *see also United States v. Villegas*, 899 F.2d 1324, 1333 (2d Cir. 1990). On a motion to suppress evidence for failure to satisfy the Fourth Amendment, then, "[t]he defendant 'bears the burden of proving . . . that he had a legitimate expectation of privacy.'" *United States v. Watson*, 404 F.3d 163, 166 (2d Cir. 2005) (quoting *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980)); *see also Rakas*, 439 U.S. at 130 n.1 ("[T]he

[2] Tellingly, Ray does not allege that the government executed the warrants with the intent or the effect of impermissibly intruding into defense strategy or into attorney-client communications. Different issues would be presented in such a case. *See, e.g.*, *United States v. Stewart*, 2002 WL 1300059 (S.D.N.Y. June 11, 2002) (describing concerns associated with searches involving likely privileged materials in search of criminal defense lawyers' offices and evaluating and outlining procedures used by courts to safeguard attorney-client privilege and Sixth Amendment right to counsel); *United States v. Neill*, 952 F. Supp. 834 (D.D.C. 1997) (explaining the "four factors . . . relevant to whether an alleged intrusion into the attorney-client privilege offends the Constitution," including whether the intrusion was intentional, in the context of materials obtained during the execution of a search warrant).

proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure."). That burden ordinarily is carried by the submission of sworn declarations. *See, e.g.*, *United States v. White*, 2018 WL 4103490, at *8 (S.D.N.Y. 2018) ("That burden 'is met only by sworn evidence, in the form of an affidavit or testimony, from the defendant or someone with personal knowledge.'") (quoting *United States v. Montoya-Eschevarria*, 892 F. Supp. 104, 106 (S.D.N.Y. 1995)).

Ray does not submit an affidavit demonstrating that he had a legitimate expectation of privacy in the Apartment, nor does he identify any other evidence that would satisfy his burden. At the time of the search, Ray had been incarcerated for almost a year and a half. The Premises Warrant itself contains evidence that the Apartment was listed in the name of Ray's father and Ray's father was posted as the tenant occupying the Apartment. Ray thus lacks standing to challenge the Premises Warrant or the search of the Premises executed pursuant to it.

Ray's argument would not withstand analysis even if he had standing. "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S 213, 232 (1983)). "The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. Moreover, "[a] magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" *Id.* at 236 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969)). "[S]o long as the magistrate had a 'substantial basis for . . . conclud[ing]' that a search would uncover

evidence of wrongdoing, the Fourth Amendment requires no more." *Id.* at 236 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

The Premises Warrant established ample probable cause both that the Computer would contain evidence of the crimes charged in the Indictment and that it would be located in the Apartment. It recited direct evidence from Female Victim-2 that a few days after Ray's arrest in February 2020, she and Pollok delivered the Computer to Ray's father at his residence and that in late December 2020, almost a year later, she saw the Computer still in the living room at the Apartment. Ray's argument that Female Victim-2 saw only the black laptop bag in December 2020 and not the Computer itself (and therefore that the presence of an undistinctive black bag is not of evidentiary value) is mistaken. Female Victim-2 told law enforcement that she saw the Computer itself in the black laptop bag.

Third, even if Ray had standing and even if the warrant did not establish probable cause, suppression would not be an appropriate remedy because law enforcement was entitled to rely in good faith on the warrant. Under the "good faith exception," the exclusionary rule and its remedy of suppression does not apply where evidence is "obtained in objectively reasonable reliance on a subsequently invalidated search warrant." *United States v. Leon*, 468 U.S. 897, 922 (1984). The law encourages law enforcement to obtain warrants and to rely upon them. Suppression of evidence obtained in reliance upon a facially valid warrant would "[p]enaliz[e] the officer for the magistrate's error" and thus not "logically contribute to the deterrence of Fourth Amendment violations." *Id.* at 921. "[S]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness," *Gates*, 462 U.S. at 267 (White, J., concurring in judgment), for "a warrant issued by a magistrate normally suffices to establish" that a law

enforcement officer has "acted in good faith in conducting the search." *United States v. Ross*, 456 U.S. 798, 823 n.32 (1982).

"'The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance' on an invalidated warrant." *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (quoting *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992)). Considering the "presumption of reasonableness" that attaches to a search pursuant to warrant, *see Clark*, 638 F.3d at 99, the Supreme Court in *Leon* identified four circumstances where the exception to the exclusionary rule does not apply: (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable, *id.* at 100 (quoting *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992)). None of those circumstances apply here. Even if there was a defect in the warrant, law enforcement was entitled to rely upon it.

Ray's challenge to law enforcement's search of the Computer also lacks merit. The Court has previously laid out the principles applicable to searches of electronic media. Under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant may "authorize the seizure of electronic storage media or the seizure or copying of electronically stored information" and "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B). "Indeed, due to the unique challenges that electronic searches pose, 'it is frequently the case with computers that the normal sequence of "search" and then selective "seizure" is turned on its head, as computer hardware is seized from a suspect's premises before its content is known and then searched at a later time.'"

United States v. Nejad, 436 F. Supp. 3d 707, 728 (S.D.N.Y. 2020) (quoting *United States v. Vilar*, 2007 WL 1075041, at *35 (S.D.N.Y. Apr. 4, 2007)); *see also United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006) (finding that officers were permitted to remove computer and storage media from the defendant's home pursuant to a search warrant "without first determining whether they actually contained child pornography"). There is thus nothing exceptional, or unconstitutional, in law enforcement's seizure of the Computer for search later at the offices of the FBI. As SA Maguire explained in the Premises Warrant, there are a number of reasons that searching a computer at a law enforcement facility is appropriate: (1) the volume of data on electronic media makes it often impractical for law enforcement personnel to review an electronic device in its entirety at the search location; (2) electronic devices are ideally examined in a controlled environment because electronic data is particularly vulnerable to inadvertent or intentional modification or destruction; (3) it can be impossible to bring to the search site all of the necessary personnel and equipment to safely access the underlying data because of the many types of electronic media currently in use; and (4) the use of passwords and encryption can complicate and prolong recovery of data from an electronic device. All or substantially all of those factors would have been at issue in this case where the Computer was password protected and it was seized in connection with a criminal case which is hotly contested and in which the defense would have every right to test whether appropriate chain of custody procedures were followed and whether the evidence from the electronic media was somehow corrupted or altered.

The search was not rendered unconstitutional because of the absence of prescribed search terms or a prescribed search methodology. As a general matter, "the warrant need not specify *how* the computers will be searched." *Vilar*, 2007 WL 1075041, at *37. It need only require the government to "reasonably limit its initial search, taking only those steps reasonably necessary to

identify documents responsive to the warrant." *United States v. Weigand*, 2020 WL 5105481, at *10 (S.D.N.Y. Aug. 31, 2020). "[O]utside the computer context, the Supreme Court has held that 'it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant.'" *Vilar*, 2007 WL 1075041, at *37 (quoting *Dalia v. United States*, 441 U.S. 238, 257 (1979)). The rule is no different when the search is to be conducted in the virtual or electronic world than in the physical world.

"The reason for not imposing such a requirement on law enforcement in conjunction with search warrant applications for computer searches is obvious—in most instances, there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities. In other words, to require courts in advance to restrict the computer search in every case to certain methodologies or terms would give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents." *United States v. Graziano*, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008). Indeed, "few people keep documents of their criminal transactions in a folder marked 'drug records.'" *Weigand*, 2020 WL 5105481, at *9 (quoting *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990)). As the Second Circuit has stated, "it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes. Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search." *United States v. Ulbricht*, 858 F.3d 71, 102 (2d Cir. 2017).

Ray argues here that the government was in possession of information from Female Victim-2 that Ray maintained separate files for the victims of the subject offenses, that he had best practices for digital folder structuring, and that he told his father that the evidence would have to be indexed and categorized. On that basis, Ray would have the Court hold that the government should be limited to searching within the Computer only those folders bearing the name of a victim. But Female Victim-2 did not say that Ray kept his documents and communications relating to the subject offense exclusively within files for the victims or that the files for the victims bore the names of the victims or any other specific identifying label. More importantly, so long as law enforcement uses reasonable measures to search electronic media and does not dwell on a non-responsive document longer than necessary to determine it is non-responsive, the Fourth Amendment's particularity requirement does not prevent law enforcement from searching the entirety of an electronic device to locate all of the evidence of criminal activity simply because it could have located some of that evidence by searching only a portion of the electronic media. "[S]earches of computers may sometimes need to be as broad as searches of residences pursuant to warrants" and, like searches for papers records, "searches for electronic records [may] entail[] the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are." *Ulbricht*, 858 F.3d at 100.

Finally, just as suppression would not be an appropriate remedy for any defects in the Premises Warrant, it would also not be an appropriate remedy even if there were defects in the Computer Warrant because the government was entitled to rely in good faith upon the terms of that warrant.

CONCLUSION

The motion to suppress is DENIED.

SO ORDERED.

Dated: November 15, 2021
New York, New York

LEWIS J. LIMAN
United States District Judge